SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, AND 30

1. REQUISITION NUMBER

PAGE 1 OF 46

2. CONTRACT NO. N65236-17-D-1005	3. AWARD/EFFECTIVE DATE 21-Dec-2016	4. ORDER NUMBER	5. SOLICITATION NUMBER N65236-15-R-0028	6. SOLICITATION ISSUE DATE 08-Nov-2016
7. FOR SOLICITATION INFORMATION CALL:	a. NAME GIANCARLO DUMENIGO		b. TELEPHONE NUMBER *(No Collect Calls)* 843-218-2375	8. OFFER DUE DATE/LOCAL TIME 02:00 PM 22 Nov 2016

9. ISSUED BY CODE N65236

US NAVY SPAWARSYSCEN ATLANTIC CHARLESTON
PO BOX 190022 2.0 CONTRACTS
843-218-2375
GIANCARLO.DUMENIGO@NAVY.MIL
NORTH CHARLESTON SC 29419-9022

TEL: 843-218-2375

FAX: 843-218-5912

10. THIS ACQUISITION IS ☒ UNRESTRICTED OR □ SET ASIDE: ______ % FOR:

□ SMALL BUSINESS

□ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM

□ HUBZONE SMALL BUSINESS

□ EDWOSB

□ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS

□ 8(A)

NAICS:
541512

SIZE STANDARD:
$27,500,000

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED

□ SEE SCHEDULE

12. DISCOUNT TERMS

□ 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION □ RFQ □ IFB ☒ RFP

15. DELIVER TO CODE

SEE SCHEDULE

16. ADMINISTERED BY CODE S0507A

DCMA LATHROP
PO BOX 232
700 EAST ROTH ROAD
BLDG 330
FRENCH CAMP CA 95231-0232

17a. CONTRACTOR/ OFFEROR CODE 63U09 FACILITY CODE

ORACLE AMERICA, INC
GOVERNMENT REPRESENTATIVE
500 ORACLE PARKWAY
REDWOOD CITY CA 94065-1677

TELEPHONE NO. 703-364-2776

18a. PAYMENT WILL BE MADE BY CODE HQ0339

DFAS-COLUMBUS CENTER
DFAS-CO/WEST ENTITLEMENT OPERATIONS
P O BOX 182381 EFT:T
COLUMBUS OH 43218-2381

□ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a. UNLESS BLOCK BELOW IS CHECKED □ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/ SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	SEE SCHEDULE				

25. ACCOUNTING AND APPROPRIATION DATA

26. TOTAL AWARD AMOUNT (For Govt. Use Only)

$45,511,729.00

□ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1. 52.212-4. FAR 52.212-3. 52.212-5 ARE ATTACHED. ADDENDA □ ARE □ ARE NOT ATTACHED

☒ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☒ ARE □ ARE NOT ATTACHED

□ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 0 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

☒ 29. AWARD OF CONTRACT: REF. OFFER DATED . YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS: SEE SCHEDULE

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

(b)(6)

30b. NAME AND TITLE OF SIGNER

(TYPE OR PRINT)

30c. DATE SIGNED

31b. NAME OF CONTRACTING OFFICER *(TYPE OR PRINT)*

Jesse Seaton / Contract Specialist
TEL: 843-218-4146
EMAIL: jesse.seaton@navy.mil

31c. DATE SIGNED

21-Dec-2016

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS (CONTINUED)		PAGE 2 OF 46

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/ SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	SEE SCHEDULE				

32a. QUANTITY IN COLUMN 21 HAS BEEN

□ RECEIVED □ INSPECTED □ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: ____________________

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
	32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER □ PARTIAL □ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT □ COMPLETE □ PARTIAL □ FINAL	37. CHECK NUMBER

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*
		42c. DATE REC'D *(YY/MM/DD)* 42d. TOTAL CONTAINERS

Pages 3 through 16 redacted for the following reasons:
- -
Not Responsive to Request

PERFORMANCE WORK STATEMENT

SPECIFICATIONS/STATEMENT OF WORK/PERFORMANCE WORK STATEMENT

Work under this performance-based contract will be performed in accordance with the following description/ specifications/ statement of work (SOW) which herein will be referred to as Performance Work Statement (PWS):

1.0 PURPOSE

1.1 BACKGROUND

The mission of Global Combat Support System Marine Corps (GCSS-MC) is to enhance the warfighter's capability by developing an integrated enterprise logistics information system that provides supply, maintenance, acquisition, transportation, health, and engineering services to Marines in deployed and garrison environments. Increment 1 allows the GCSS-MC Program Management Office (PMO) and system to provide asset visibility, supply, maintenance, readiness, and financial information for garrison and deployed operations. The organization charged with supporting, operating, and maintaining this next generation logistics warfighter capability is the GCSS-MC PMO.

This effort is a follow-on to Contract N65236-13-D-2157. Oracle's E-Business Suite and tools were acquired in August 2004 using a competitive source selection process managed by the Marine Corps Systems Command (MCSC). During January 2006, the program elected to leverage its strategic partnership with Oracle to complete the Global Combat Support System Marine Corps (GCSS-MC) Increment 1 solution. Oracle has provided system integration and development services for the GCSS-MC system since that time.

1.2 SCOPE

The contractor will provide post deployment systems support (PDSS) for Increment 1 of Global Combat Support - Marine Corps (GCSS-MC). This specific contract action will provide continued PDSS/ sustainment and the delivery of Release 1.1+ capabilities.

PDSS Sustainment will include Tier 3 Help Desk Support to resolve user reported system discrepancies. This includes but is not limited to completing Priority 1 and 2 Change Requests and supporting the installation of Cyber Command Information Assurance Vulnerability Assessment (IAVA) security patches. Release 1.1+ will provide GCSS-MC Increment 1 functionality in austere communication environments associated with deployed Marine Air-Ground Task Force (MAGTF) operations and exercises.

2.0 APPLICABLE DOCUMENTS (AND DEFINITIONS)

The contractor shall ensure all work accomplished on task utilizes the best commercial practices and current acceptable industry standards. The applicable references and standards invoked will vary within individual tasks and will be specifically called-out in each task order. In accordance with Defense Acquisition Policy changes, maximum utilization of non-Government standards, as embodied by the standard of best commercial practices and current acceptable industry standards, will be made to the documents listed in 2.1 and 2.2 below wherever practical. Where backward compatibility with existing systems is required, selected interoperability standards will be invoked. For proposal purposes, the following documents are not exclusive; however, except as noted above and stated in the contractor's proposal, all contractors shall be able to meet those cited when applicable to the task order.

2.1 REQUIRED DOCUMENTS

The following instructional documents as specifically referenced in text of Task Order requirements are mandatory for use. Unless otherwise specified, the document's effective date of issue is the date on the request for proposal. Additional applicable documents may be included in specific task orders as mutually agreed to by the parties.

	Document Number	Title	Section of

			PWS
a.	DoD 5200.2-R	DoD Regulation – Personnel Security Program dtd Jan 87	8.2.2.4 (a), 8.2.3
b.	DoDM 5200.01	DoD Manual – Information Security Program Manual dtd 24 Feb 12	7.3.2, 7.3.2.2
c.	DoDD 5205.02E	DoD Directive – Operations Security (OPSEC) Program dtd 20 Jun 12	8.3
d.	DoD 5205.02-M	DoD Manual – Operations Security (OPSEC) Program Manual dtd 3 Nov 08	8.3
e.	DoD 5220.22-M	DoD Manual – National Industrial Security Program Operating Manual (NISPOM) dtd 28 Feb 06	8.2, 8.2.2.1, 8.2.4
f.	DoDI 5220.22	DoD Instruction – National Industrial Security Program dtd 18 Mar 11	8.2
g.	DoDI 8500.01	DoD Instruction – Cybersecurity dtd 14 Mar 14	8.2.1, 8.2.3
h.	DoDI 8510.01	DoD Instruction – Risk Management Framework (RMF) for DoD Information Technology (IT) dtd 12 Mar 14	4.1.2, 4.1.5
i.	DoD 8570.01-M	Information Assurance Workforce Improvement Program dtd 19 Dec 05 with Change 3 dtd 24 Jan 12	5.2.1.3, 8.2, 8.2.3
j.	DoDD 8570.01	DoD Directive – Information Assurance Training, Certification, and Workforce Management dtd 15 Aug 04	5.2.1.3, 8.2,8. 8.2.3
k.	SECNAV M-5239.2	DON Information Assurance Workforce Management Manual dtd May 2009	8.2.3
l.	SECNAV M-5510.30	Secretary of the Navy Manual – DoN Personnel Security Program dtd Jun 2006	8.2.3
m.	SECNAVINST 5239.3B	DoN Information Assurance Policy, 17 Jun 09	4.1.5
n.	SECNAVINST 5510.30	DoN Regulation – Personnel Security Program	8.2, 8.2.3

2.2 GUIDANCE DOCUMENTS

The following documents are to be used as guidance as may be included in specific requests for proposals. Unless otherwise specified, the document's effective date of issue is the date on the request for proposal. Additional applicable documents may be included in specific task orders.

	Document Number	**Title**	**Section of PWS**
a.	DoDI 4151.19	DoD Instruction – Serialized Item Management (SIM) for Life-Cycle Management of Materiel, 9 Jan 14	11.2.4
b.	DoDI 4161.02	DoD Instruction – Accountability and Management of Government Contract Property, 27 Apr 12	11.2.3
c.	HSPD-12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004	8.2.2.3
d.	DoDM-1000.13-M-V1	DoD Manual – DoD Identification Cards: ID card Life-Cycle dtd 23 Jan 14	8.2.2.4 (a) and (b)
e.	FIPS PUB 201-2	Federal Information Processing Standards Publication 201-2 – Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013	8.2.2.4 (a) 3
f.	Form I-9, OMB No. 115-0136	US Department of Justice, Immigration and Naturalization Services, Form I-9, OMB No. 115-0136 – Employment Eligibility Verification	8.2.2.4 (a)

2.3 SOURCE OF DOCUMENTS

The contractor shall obtain all applicable documents. Many documents are available from online sources. Specifications and commercial/industrial documents may be obtained from the following sources:

Copies of Federal Specifications may be obtained from General Services Administration Offices in Washington, DC, Seattle, San Francisco, Denver, Kansas City, MO., Chicago, Atlanta, New York, Boston, Dallas and Los Angeles.

Copies of military specifications may be obtained from the Commanding Officer, Naval Supply Depot, 3801 Tabor Avenue, Philadelphia, PA 19120-5099. Application for copies of other Military Documents should be addressed to Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Ave., Philadelphia, PA 19120-5099.

All other commercial and industrial documents can be obtained through the respective organization's website.

3.0 PERFORMANCE REQUIREMENTS

The following paragraphs list all required support tasks that may be required throughout the contract life. The contractor shall provide necessary resources and knowledge to support the listed tasks. Specific objectives will be dependent on the IDIQ contract and the task order (TO) as may be written against the IDIQ contract. The contractor shall complete all required tasks as may be included in the TO while controlling and tracking performance and goals in terms of costs, schedules, and resources.

The list below outlines support tasks that shall be required throughout the contract life:

- The Contractor shall operate as a consulting partner and shall work directly with GCSS-MC PMO and SPAWARSYSCEN ATLANTIC engineers to perform all aspects of the PWS.

- The Contractor shall work with the GCSS-MC PMO and SSC Atlantic to accomplish the sharing of system knowledge to the GCSS-MC Government Team. All knowledge sharing deliverables developed shall be provided to GCSS-MC PMO and SPAWAR.

- The Contractor shall provide documentation about the work performed, including installation and configuration instructions, maintenance processes and procedures, physical and logical infrastructure diagrams, Reports, Interfaces, Customizations and Extensions (RICE) object requirements and designs, knowledgebase and configuration management system updates regarding system changes.

- The Contractor shall provide documentation for design, development, testing, installing, supporting, and maintaining the GCSS-MC LCM system.

- The Contractor shall provide personnel experienced in the development, maintenance and sustainment of the GCSS-MC portfolio of systems.

- The Contractor shall execute modular development activities in an effort to minimize dependencies between capabilities.

- The Contractor shall reference the Systems Engineering Management Plan for Priority 1 and 2 deficiency definitions.

- The Contractor shall provide Technical Leads.

- The Contractor shall supply technical documentation updates in accordance with the approved CM process.

3.1 TECHNICAL AND ENGINEERING SUPPORT

The Government intends to continue plans to upgrade to R12 EBS. The Contractor shall provide engineering and logistics integration support services in support of GCSS-MC PMO, Configuration Control Board and Release Management planning priorities.

3.1.1 Deliverables

The Contractor shall deliver products and/or services as detailed in the Task Order.

3.2 PROJECT MANAGEMENT

The Contractor shall perform planning, execution, management, monitoring and control activities in support of the requirements of this contract. The Contractor shall:

- Assist the Government in Program/Project Planning to develop and report financial and schedule information, as well as report deficiencies and identify critical path.

- Conduct resource management, establish priorities and make recommendations in assigning priorities and allocating resources.

- Assess risks and issues, provide tracking and escalate risks and issues

- Identify monitoring, feedback and process controls mechanisms to measure effectiveness in achieving contract and task order milestones and deliverables.

- Produce, track and maintain programmatic, software, performance, and system metrics.

- Verify that required business operations data is obtained, kept current and made available to all disciplines.

- Develop and maintain project documentation in support of the contract.

- Prepare for and participate in project meetings and status reviews and other meetings.

- Assist in the development and refine the clarity of requirements and deliverables.

- Lead day-to-day, on-site staff work – maintaining situational awareness internally and Externally.

- Participate in meetings and collaborate with GCSS-MC PMO, SSC Atlantic and its industry partners.

3.2.1 Deliverables

The Contractor shall deliver products and /or services with supporting technical documentation, including the following as applicable per the TO:

- Monthly Status Report
- Program Management Reporting & Metrics (CDRL A001)
- Application Software Metrics
- Monthly Change Request Summary
- Plan of Action & Milestones
- Risk and Issue Tracking Report
- Travel Reports (when requested)
- PSR and other briefs
- Project documentation to include technical deliverables

3.3 SUSTAINMENT

3.3.1 Software Development Support

The Contractor shall:

- Sustain and maintain the software architecture, engineering, development, data staging, testing and configuration of the Software Development Environment (SDE). Activities shall include documented digital and verbal communication, as well as team participation.

- Share information about the RICE development methodologies; including the RICE components/modules and architecture, toolsets, and integration testing plans; data staging and test results and technical documentation.

- Provide problem management services that relate to reported or discovered incidents and problems.

- Provide visibility of Contractor standards of coding practice prior to promoting the code into configuration-managed environments.

- Provide GCSS-MC functional application support and testing.

- Support and follow the Government testing and configuration management processes for all software releases.

- Work with the Lead Engineer and his staff to develop functional design solutions for change requests.

- Develop both unit and integration test plans for use by both the CR functional tester and Government testers for change requests and any code changes.

- Provide SME / Analyst input to functional design change requests.

- Support Government testers and resolve issues.

- Develop or modify test cases and scripts for specific scenarios to test bug fixes or change requests.

- Develop and document unit and regression test scripts and document results.

3.3.2 Work Items & Engineering Change Proposals

The Contractor shall perform the following activities relating to Work Items and / or Engineering Change Proposals:

- Comply with the GCSS-MC configuration control and change management processes.

- Perform duties that provide a review of the LOE and scope against specific, proposed functional system changes that require a technical solution. If more than one estimate is required (e.g., multiple Courses of Action [COAs]), the COR will be made aware of the LOE associated with each possible COA determination.

- Provide an estimate toward what is considered the best COA.

- Review and validate each Critical Patch Update (CPU) to determine its effect on GCSS-MC specific RICE elements.

- Provide an RICE impact assessment of the CPU. This impact analysis shall include an LOE to modify RICE element for CPU, after the regression test

- If directed, the Contractor shall perform work associated with approved LOE

- Support and collaborate with Government Functional Leads on the capability of Oracle solutions to address Functional Requirements.

- Supply an overview and detailed functional fit analysis of the commercially available standard solution against the GCSS-MC functional requirement.

- Develop technical design specifications for approved system enhancements

3.3.2.1 Deliverables

The Contractor shall deliver products and /or services with supporting technical documentation as may be required in the Task Order.

3.3.3 Engineering Support

The Contractor shall:

- Support integration and apply CYBER Command Information Assurance Vulnerability Alert (IAVA) patches.

- Support access to development environments as by PM GCSS-MC and SSC Atlantic.

- Execute technical direction for the development, design and integration for custom designed products as directed by the COR.

- Support the maintenance of a conversion staging environment as a part of system sustainment currently in support of the LIS (Logistics Information Systems) Team in Albany, GA

3.3.3.1 Deliverables

The Contractor shall deliver products and /or services with supporting technical documentation, including the following as may be contained in a Task Order (CDRL A002):

- Module Design & Build documentation

- Technical Data Package (TDP) Input

- Reports, Interfaces, Customizations and Extensions (RICE) Objects Inter-relationship Diagram

- Provide STIG/SRR reports to Information Assurance team members

- Support and provide the data needed for Government analysis of Mean Time to Change (MTTC).
- Support GCSS-MC PMO with Root Cause Analysis (RCA)

- Oracle Unified Method (OUM)/Application Implementation Methodology (AIM) Document Updates

3.3.4 Enterprise Training Program Support

The Enterprise Training Program (ETP) support consists of the development and delivery of GCSS-MC Training courseware and materials. The GCSS-MC ETP also includes training materials housed at the Marine Corps Training and Education (TECOM) Formal Learning Centers (FLC) and the Marine Expeditionary Force (MEF) Materiel Readiness Centers (MRTC). The FLCs possess training materials (Supply, Maintenance, and Finance) military occupational specialty entry-level and career-level courseware. The MRTC possesses Mobile Training Suites and training materials to support MEF supply, maintenance, and financial supply and maintenance activities. As defined at the task order level, the Contractor shall:

- Provide personnel that possess Oracle Applications Database Administrator (DBA) experience.

- Provide personnel that possess Oracle EBS experience.

- Provide EBS specialists, and Application DBAs at GCSS-MC training locations as required by the TO.

- Troubleshoot any MTS/RTS equipment requiring maintenance, and maintain training environment/suite hardware; software warranty actions, and repair/replace as required.

- Maintain and update MTS/RTS customized menu scripts, processes, and procedures for data and environment backups/restore procedures.

- Conduct training builds for migration of courseware from production to developer's Environment.

.

- Maintain, support and provide curriculum developers access to training developmental environments and file shares.

3.3.4.1 Deliverables

The Contractor shall deliver products and /or services with supporting technical documentation, including the following as may be contained in a Task Order:

- OUM / AIM Document Updates

- Provide training support for Non-Production Solution Development Environment at the Carpathia hosting facility.

- Training materials and technical documentation.

3.3.5 Life Cycle Support Engineering Services

As may be contained in a TO, the Contractor shall:

- Research emerging technologies as approved by the Government to make recommendations to provide benefit to the GCSS-MC.

- Update Solution Design and Build Deliverables (RICE and Non-RICE) inclusive in the design documentation Requirement Traceability Matrix (RTM) sections.

- Provide analysis, recommendations and technical risk assessment for system modifications, upgrades and routine system maintenance activities.

- Provide the strategy and design of the Enterprise Solution Architecture, and assure integrity of the Technical Solution.

- Provide software end-of-support and new release information and recommendations. Recommendations should include technical refresh strategies in order to maintain Oracle support, coverage and compliance.

- Manage technical risks;

    - shall identify and document technical risk,

    - work with Government to capture and quantify the potential impact of the risk,

    - assist in defining mitigation techniques,

    - participate in risk reviews.

- Complete any setups necessary to implement business process change or code fix.

- Resolve and/or escalate issues in a timely manner per the awarded task order.
- Support data calls and extracts required for Certifications.
- Utilize tools agreed to or implemented by the Government.
- Work with the Lead Engineer and his staff to define, document, and implement applicable Government approved lifecycle engineering processes and tools in support of GCSS-MC.
- Adhere to and provide improvement recommendations for applicable Government approved lifecycle engineering processes and tools in support of the Lead Engineer and his staff.
- Provide support and material input for required systems engineering technical reviews (SETR) processes and events.

3.3.5.2 Audit Readiness

GCSS-MC will be assessed via an Audit Readiness review. The audits within the 2011 Financial Improvement Audit Readiness (FIAR) are divided into the control areas below.

1. Access Control
2. Security Management
3. Configuration Management
4. Separation of Duties
5. Contingency Planning
6. Business Process Controls
7. Interface Controls
8. Data Management System Controls

The control areas are divided into 11 assessable units (i.e., checklists) with a potential for 2 additional checklists for Existence and Completeness (E&C) as listed below.

1. Contract Pay
2. Supplies (MILSTRIP)
3. Vendor Pay
4. Reimbursable Work Order – Grantor
5. Fund Balance with Treasury
6. Appropriations Received
7. Military Pay
8. Civilian pay
9. Reimbursable Work Order – Acceptor
10. Other Budgetary Activity
11. Financial Reporting
12. Inventory (E&C)
13. Operating Materials and Supplies (E&C)

The Contractor shall provide support in decomposing requirements and developing the Plan of Action and Milestones (POA&M) as reqiured in the TO to achieve financial compliance.

3.3.6 RESERVED

3.3.7 Non-Production Site Support (Carpathia)

The Contractor shall continue supporting the Carpathia environment, including Infrastructure and applications so the environment is available for continuous development in support of the current production system until such time the Government provides direction to decommission. As may be contained in a task order, the Contractor shall:

- Provide a single point of contact for the SDE

- Provide a strategy for decommission of Carpathia and implement decommission upon Government approval

- Provide development and test support.

- Provide technical planning and assistance to service requests.

- Provide details of service requests, current status of requests, and action items for completion.

- Provide assistance with installation and configuration questions.

- Provide onsite touch labor support to physically resolve identified faults per Government direction.

3.3.8 Deliverables

The Contractor shall deliver products and /or services with supporting technical documentation, including the following as may be contained in a task order:

- OUM / AIM Document Updates

3.3.9 Information Assurance / Cyber Security

Information Assurance (IA) includes tasks which the Contractor shall protect and defend information and information systems by verifying their availability, integrity, authentication, confidentiality, and non-repudiation.

3.3.9.1 General Cyber Security Support

The Contractor shall support continued Cyber-Security system security, accreditation, user administration, and application security testing in accordance with public laws and Chairman of the Joint Chief of Staff, Department of Defense (DoD), Department of the Navy (DoN), U.S. Marine Corps (USMC), and Marine Corps Systems Command policy, guidance standards, and standardized process and procedures.

The Contractor shall as may be contained in a task order:

- Create and update service tickets within the SSC Atlantic approved ticket management system to include the identification, modifications and corrections.

- Support GCSS-MC PMO office by following the Incident Response Plan (IRP) for all incidents within the Production Environment (Government Operations Center (GOC) Support) and Development Environment (SDEs)).

- Assist with the development/modification of the applicable GCSS-MC system role/responsibilities.

- Verify appropriate Trading Community Relationships in Read Only Mode.

- Support GCSS-MC PMO in establishing approval groups in Oracle Access Manager.

- Support GCSS-MC PMO in quarterly system security readiness reviews to verify DoD Security Technical Implementation Guidance (STIG).

- Support GCSS-MC PMO in correcting findings identified during quarterly security readiness reviews and Oracle code reviews.

- Support GCSS-MC PMO in complying with USCYBERCOM directed actions thru the application and reporting of applicable Information Assurance Vulnerability Alerts and Bulletins on GCSS-MC system and subsystem components.

- Support GCSS-MC PMO in the application of build/emergency/patch sets to development environments in accordance with Configuration Management sequencing.

3.3.9.2 Deliverables

The Contractor shall deliver products and /or services with supporting technical documentation, including the following as may be contained in a Task Order (CDRL A002):

- Updated POA&M sheet following remediation activities.

- Recommendations to vulnerability findings. (Security POA&M)

- Ticket Resolution

- OUM / AIM Document Updates

3.3.10 Post Deployment Support System – Production

PDSS services focus on system operation, maintenance, application, and infrastructure sustainment. The Contractor will perform tasks required in the support of the Government-run GOC.

- The Contractor shall provide skill-sets necessary to sustain and maintain the GCSS-MC LCM application, and associated capabilities.

- The Contractor shall provide skill sets and experience to sustain the maintenance of the GCSS-MC System PDSS environments.

3.3.10.1 Tier 3 Service Desk

The GCSS-MC Tier 3 Service Desk receives trouble tickets and Service Requests (SRs) that may not be resolved at the T2 Service Desk and provides functional and technical support, consultation, and services to GCSS-MC PMO PDSS Lead. The Contractor shall provide staff with experience in systems administration, database administration, interface management, system analysis, and other skill sets necessary to develop and provide timely and effective responses to operational or technical problems or issues that may arise during system operation and maintenance.

3.3.10.1.1 Tier 3 Help Desk Activities

The Contractor shall support GCSS-MC PMO with the following tasks:

- Identify issues which cannot be addressed at the T3 level and which require vendor or hosting site resolution and forward to the appropriate entity for reconciliation and corrective action.

- Analyze and provide support for Workflow processes and problems.

- Update SRs in SSC Atlantic Remedy system. This system will be used to generate automated reports as required by PMO.

- Submit Knowledge Base (KB) articles for approval by the PMO SME group via the GCSS-MC Training Resource Manager (TRM) and the workflow process.

- Make enhancement recommendations via the CCB process that may provide more effective use or reduce maintenance costs for the GCSS-MC system.

- Report issues that require Oracle COTS enhancements to GCSS-MC PDSS Manager/Designate for escalation to the CCB.

- Monitor system integrity and usability in accordance with the current metrics requirements

- Perform Root Cause Analysis (RCA) for P1 and P2 issues.

- The Contractor shall develop a RCA report for problem management issues.

    - The Contractor shall provide status updates during RCA.
    - The Contractor shall provide a final report within 72 hours of problem resolution in a Government-approved format.

- Analyze and research issues forwarded to Tier 3 by Tier 2.

- Notify the GCSS-MC PMO Manager/Designate when a system notification is warranted.

- Perform those duties associated with incident management, to include the review of an incident, testing, documentation, reporting, and promotion of the fix, followed by proper closure of the trouble ticket/SR.

3.3.10.1.2 Tier 3 Service Desk Deliverables
The Contractor shall deliver products and /or services with supporting technical documentation, including the following (CDRL A002):

- SRs
- KB Articles
- CRs
- ECPs
- RCA Report

3.3.10.1.3 Tier 3 On-Call or Extended Shift Requirements
In the event of a problem, application, or system outage requiring immediate attention, Hosting Site interface or coordination, or an initial fielding requirement, the Contractor supporting T3 shall be available to work extended hours to perform these mission essential tasks as directed by the contracting officer or his/her designated representative.

- An on-call requirement necessitates that the Contractor be available within a 2-hour window to perform a required task through its resolution.

- An extended shift requirement is the requirement for the Contractor to remain engaged on a problem, application, or system outage requiring immediate resolution, Hosting Site interface or coordination, or an initial fielding requirement until the aforementioned are addressed.

- In the event of a scheduled or unscheduled outage, Contractor must notify GCSS-MC PMO PDSS Manager/Designate for approval.

3.3.10.2 Tier 3 Operations
These tasks pertain to providing PDSS services that focus on operation, maintenance, and application sustainment efforts. This consists of updating system software and database configuration items.

3.3.10.2.1 System Maintenance and Operational Support Activities
The Contractor shall support GCSS-MC PMO in the performance of the following System Maintenance and Operational Support functions:

- Analyze recurring unscheduled outages and propose improvements to the environments to increase availability.

- Coordinate scheduled outages for the environments with the Government per a mutually agreed upon process.

- Startup and shutdown Oracle programs in the environments.

- Install Oracle monitoring tools on GCSS-MC servers, or use GCSS-MC existing monitoring tool set as determined by the Government.

- Detect, acknowledge, and notify Tier 1 and the GOC Manager/Designate of system outages.

- Initiate incident management process pursuant to service restoration.

- Facilitate configuration of monitoring events.

- Provide data in the area of Operating System (OS) performance graphs, upon request, where such data is available.

- Apply build/emergency/patch sets to Production Support System (PSS) and Production.

- Review, monitor, and apply IAVAs as required for database and applications impacts and promote the changes to production following CM procedures.

- Facilitate LINUX Kernel Upgrade as per IAVA with DISA on PSS and Production.

- 24X7 support for Cut Over activities.

- Support for F5 Load Balancer Technical Issues.

- Provide weekly and on-demand backups.

- Maintain Servers – file systems, user password maintenance, and security.

- Provide content for User notifications, including attachments if applicable to the Tier-3 team.

- Identify system event thresholds and implement proactive response alerts.

- Monitor and respond to system alerts - 24X7.

- Perform preventive action on Grid control alerts which warrant an action from the team.

- Provide network support among servers.

- Provide DBA support for install and troubleshooting of Mobile Field Services (MFS).

- Provide DBA support for legacy interfaces issues and troubleshooting.

- Provide DBA support to Information Assurance (IA) team to install and assist promoting the standard and customized code to production.

- Provide GCSS-MC environment cloning support.

- Maintain database integrity and apply EBS patches

- Install, maintain, and configure the Real Application Clusters (RAC), Automatic Storage Management (ASM), and Cluster Ready Services (CRS) on Linux or latest revisions as applicable.

- Apply Interoperability patches between latest revisions as applicable.

- Install, configure, and maintain Oracle Lite and Mobile Server as directed by the Government.

- Administer Business Intelligence and Discoverer Admin, Plus, and Viewer.

- Install, configure, administer, and maintain Business Process Execution Language (BPEL) / Service Oriented Architecture (SOA) as directed by the Government.

- Install, maintain, and administer B2B Server and Discoverer with Oracle EBS.

- Maintain Transparent Data Encryption (TDE), SSL, and PKI for Oracle Applications.

- Conduct testing for patches and fixes.

- Support instance refreshes.

- Execute unit, regression, and backup and recovery testing.

- Provide feedback to developers on failed test cases.

3.3.10.2.2 Capacity Management Activities
The Contractor shall perform Capacity Management actions. For the purpose of this effort, capacity management encompasses the current and future capacity and performance considerations for the database environments. Specifically, the Contractor shall:

- Administer schema objects.
  - o Create and maintain schema objects.
  - o Grant privileges, as specified by GCSS-MC IAM, on objects either to pre-defined roles (which will then be granted to database users) or directly to user accounts.
  - o Monitor the growth of the database segments and address any fragmentation issues as necessary.

- Create and maintain database links to the environments.

- Perform table and/or table space defragmentation operations.
  - Administer space usage for table spaces within the environments. Provide performance tuning and maintenance of the environments as follows:

    - o Rebuild indexes
    - o Reorganize table spaces
    - o Gather schema statistics
    - o Redistribute data files
    - o Adjust Oracle "init.ora" database parameters
    - o Propose, to the GOC Manager/Designate, operating system changes pursuant to performance of the environments

- Provide performance and tuning for Oracle database, Application & Discoverer reports

- Perform incident diagnoses and follow-up in the environments as follows: o Analyze and diagnose performance issues with the Oracle databases

  - o Analyze and diagnose performance issues with the Oracle databases
  - o Generate and log an SR with Oracle America, Inc.
  - o Facilitate the analysis of Trouble Tickets and SRs
  - o Create database trace files

- Provide a weekly GCSS-MC Enterprise NIPRNet Capacity Report (CDRL-A002) that includes:
    - Information related to service, resource utilization, and performance.
    - A capacity plan that documents current utilization and forecasted requirements and an annual infrastructure capacity growth plan.

- Prepare white papers that clearly address technical and functional issues.

3.3.10.2.3 Tier 3 Operations Deliverables
The Contractor shall deliver products and /or services with supporting technical documentation, including the following (CDRL A002):

- Availability Improvement Proposals
- System Outage Notifications
- OS Performance Graphs
- Script updates and guidelines (to accomplish changes which involve the load balancer)
- Weekly and On-Demand Backups
- New System Alerts
- Environment Clones
- SRs
- Database Trace Files
- NIPRNet Capacity Report
- Technical and Functional White Papers as directed by the Government

3.3.10.3 Tier 3 Interfaces / Middleware

3.3.10.3.1 Tier 3 Interfaces / Middleware Activities
The Contractor shall support GCSS-MC PMO in the performance of the following actions related to the Oracle Application Middleware Suite:

- Monitor server domains, application servers, clusters, Java components, system components, and applications; report and address service interruptions.

- Monitor workflow and apprise the SSC Atlantic GOC Manager of any failed messages.

- Monitor the BPEL dehydration store.

- Monitor the metadata repository.

- Monitor Java Virtual Machines.

- Monitor limit for connection pools.

- Monitor transaction rollbacks.

- Monitor logs for errors and performance issues.

- Monitor business activity via the business activity dashboard.

- Monitor the BPEL console process logs.

- Monitor Business to Business (B2B) console and error message report.

- Monitor Oracle Web Service Manager’s (OWSM’s) message logs and reports.

- Monitor B2B Server logs and report.

- Monitor the File Transfer Protocol / Secure File Transfer Protocol directory space usage.

- Monitor the BPEL queues for unprocessed messages.

- Manage the metadata repository per the database capacity management criteria where such metadata repository is database-based.

- Manage the BPEL dehydration store per the database capacity management criteria.

- Reconfigure Oracle Fusion Middleware and Java components as required to maintain performance.

- Identify applications with poor performance or inordinate resource requirements.

- Provide Staging Table Interface Extracts to be utilized for Analysis.

- Provide Runtime Analysis of Concurrent Processes.

- Proactively monitor EBS Production System.

- Support technical aspects of functional user testing.

- Provide artifacts to identify characteristics of all interfaces to include architectural diagrams

3.3.10.3.2 Tier 3 Interfaces / Middleware Deliverables
The Contractor shall deliver products and /or services with supporting technical documentation, including the following (CDRL A002):

- Service Interruption Reports
- SRs
- Staging Table Interface Extracts
- Runtime Analysis of Concurrent Processes
- Architectural Diagrams

3.3.10.4 Tier 3 Business Systems Integration (BSI)
The Contractor shall provide full time equivalent personnel to support data cleansing activities, reporting to legacy system owners, and fulfillment of the following:

3.3.10.4.1 Data Integration and System Support Activities

- Support continued data integration activities, which are cross-matrixed in support of version 1.1.1, PDSS, and new capabilities.

- Connect and maintain integration of the GCSS-MC system with external systems.

- Support the BSI Team with external interface support and coordination.

- Using the understanding of the functional and technical processes of the system, assist in the categorization and prioritization of BSI issues.

- Propose solutions relating to issues involving data exchanges.

- Maintain the customization documentation to support architecture and design reviews.

- Support BSI testing activities in various support areas not limited to these: queries and script execution, XML, eXML & SOAP messages, SFTP & HTTPS, B2B, and DLMS & Federal EDI standard, Workflow, performance analysis tuning.

3.3.10.4.2 Data Quality Management Activities

- Provide support for data quality activities.
  - Evaluate data quality for the data quality dimensions applicable to the issue. The assessment results provide a basis for future steps, such as identifying root causes and needed improvements and data corrections
  - Using a variety of techniques, determine the impact of poor quality data on the business. This provides input to establish the business case for improvement, to gain support for data quality, and to determine appropriate investments
  - Prioritize the true causes of the data quality problems and develop specific recommendations for addressing them.
  - Monitor interface and conversion performance for data quality impacts.
- Log data quality issues as SRs and properly categorize, route, and track for resolution.
- Upon approval, implement steps to make appropriate data corrections through mass updates while coordinating activities across PMO and BSI developers (automated)
- Monitor the execution of customizations within the system's architecture framework and develop management metrics, with primary focus on external data exchanges.
- Provide a monthly report of data quality issues, to include source, impact, and corrective action.

3.3.10.4.3 Tier 3 BSI Deliverables

The Contractor shall perform all Government-established GCSS-MC test practices to support the full documentation of test plans, test scripts, test cases, test episodes and test results developed by the Contractor in support of their Contractor verification test phases and Government test phases (CDRL A002).

3.4 OAM

The Contractor shall:

- Install and configure up Oracle Application Management Suite - Identify Management Pack in the Solution Development Environment.
- Demonstrate Oracle Application Management Suite - Identity Management pack to stakeholders for the purpose of understanding product capabilities and proper usage applied to GCSS-MC.
- Develop POA&M for full implementation to be described in future task orders

4.0 INFORMATION TECHNOLOGY (IT) SERVICES REQUIREMENTS

4.1 INFORMATION TECHNOLOGY (IT) GENERAL REQUIREMENTS

When applicable, the contractor shall be responsible for the following:

4.1.1 Ensure that no production systems are operational on any RDT&E network.

4.1.2 Follow DoDI 8510.01 of 12 Mar 2014 when deploying, integrating, and implementing IT capabilities.

4.1.4 Work with Government personnel to ensure Navy's compliance with all current Navy IT & cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).

4.1.5 Follow SECNAVINST 5239.3B of 17 June 2009 & DoDI 8510.01 of 12 Mar 2014 prior to integration and implementation of IT solutions or systems.

4.2 ACQUISITION OF COMMERCIAL SOFTWARE PRODUCTS, HARDWARE, AND RELATED SERVICES

Contractors recommending or purchasing commercial software products, hardware, and related services supporting Navy programs and projects shall ensure they recommend or procure items from approved sources in accordance with the latest DoN and DoD policies.

5.0 CONTRACT ADMINISTRATION

Contract administration is required for all contracts; it provides the Government a means for contract management and monitoring. Regardless of the level of support, the ultimate objective of the contractor is ensuring the Government's requirements are met, delivered on schedule, and performed within budget.

5.1 CONTRACT LIAISON

The contractor shall assign a technical single point of contact, also known as the Program Manager (PM) who shall work closely with the Government PM. The contractor PM, located in the contractor's facility, shall be responsible for ensuring that the contractor's performance meets all Government contracting requirements pertaining to price and schedule. The PM shall have access to those company resources necessary for contract performance. The PM shall be responsible for the following: contractor program personnel management; management of Government owned or provided material and assets to the contractor; and contractor personnel and contractor facility security.

The contractor shall assign a contractual single point of contact, also known as the Contract Liaison, to work with the Government's Contracting Officer and Contracting Officer's Representative (COR). CORs will be assigned at the task order level. In support of open communication, the Contract Liaison shall initiate, unless otherwise directed at the task order level, periodic meetings with the COR.

5.2 CONTRACT MONITORING AND MAINTENANCE

5.2.1 <u>Contract Administration Documentation</u>
Various types of contract administration documents are required throughout the life of the contract. At a minimum, the contractor shall provide the following documentation, unless otherwise specified:

5.2.1.1 Task Order Status Report
The contractor shall develop a Task Order Status Reports (TOSR) (CDRL A005) and submit it monthly. The Status Reports include the following variations of reports:

(a) Monthly TOSR – the contractor shall develop and submit a TOSR monthly at least 30 days after TO award on the 10th of each month for those months the is active. The contractor shall report on various TO functions: performance, schedule, financial, business relations, and staffing plan/key personnel; see applicable DD Form 1423 for additional reporting details and distribution instructions. This CDRL includes a Staffing Plan (Attachment 1), Personnel Listing (Attachment 2), and Government Furnished Property (GFP) Template (Attachment 3) necessary for additional data collection as applicable.

(b) Data Calls – the contractor shall develop and submit a data call report which is e-mailed to the COR within six working hours of the request, unless otherwise specified by TO. The contractor shall ensure all information provided is the most current. Funding data will reflect real-time balances. Report will account for all planned, obligated, and expended charges and hours. At a minimum unless otherwise noted, the contractor shall include in the data call the following items and data:

1. Percentage of work completed
2. Percentage of funds expended
3. Updates to the POA&M and narratives to explain any variances
4. List of personnel (by location, security clearance, quantity)
5. Most current GFP and/or CAP listing

5.2.1.2 Task Order Closeout Report

The contractor shall develop a task order (TO) closeout report (CDRL A006) and submit it no later than 15 days before the TO completion date. The Prime shall be responsible for collecting, integrating, and reporting all subcontracting information. See applicable DD Form 1423 for additional reporting details and distribution instructions.

5.2.1.3 Cybersecurity Workforce (CSWF) Report

DoD 8570.01-M and DFAR's PGI 239.7102-3 have promulgated that contractor personnel shall have documented current cybersecurity certification status within their contract. The contractor shall develop, maintain, and submit a CSWF Report (CDRL A004) monthly or as applicable at the task order level (Note: If initiated at the TO level, report not necessary at contract level). IAW clause DFARS 252.239-7001, if cybersecurity support is provided, the contractor shall provide a Cybersecurity Workforce (CSWF) list that identifies those individuals who are IA trained and certified. Utilizing the format provided in CSWF CDRL Attachment 1, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Contractor shall verify with the COR or other Government representative the proper labor category cybersecurity designation and certification requirements.

5.2.1.4 Contractor Manpower Reporting

The following reporting is required for all DoD contracts acquiring services regardless if cost type or firm-fixed price contract:

(a) Contractor Manpower Quarterly Status Report (QSR)

The contractor shall provide a Contractor Manpower Quarterly Status Report (CDRL A004) to GCSS-MC PMO four times throughout the calendar year. Required by GCSS-MC PMO for all active service contracts/TOs (regardless if fixed-price or cost type), the Manpower report itemizes specific contract and/or TO administrative data for GCSS-PMO. Reporting period begins at the time of contract/TO award. Utilizing the format provided in QSR CDRL Attachment 1, the contractor shall collect required data throughout the specified performance period and shall submit one cumulative report on the applicable quarterly due date. See applicable DD Form 1423 for additional reporting details and distribution instructions. The following table lists the pre-set submittal due dates and the corresponding performance periods:

#	QUARTERLY DUE DATE	PERFORMANCE PERIOD
1	15 January	1 October – 31 December
2	15 April	1 January – 31 March
3	15 July	1 April – 30 June
4	15 Oct	1 July – 30 September

(b) Enterprise-wide Contractor Manpower Reporting Application

In addition to the QSR CDRL reporting requirements noted above and pursuant to NMCARS 5237.102-90, the contractor shall report all contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the DoD via a secure data collection website – Enterprise-wide Contractor Manpower Reporting Application (eCMRA). Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

(1) W, Lease/Rental of Equipment;
(2) X, Lease/Rental of Facilities;
(3) Y, Construction of Structures and Facilities;

(4) S, Utilities ONLY;
(5) V, Freight and Shipping ONLY.

The contractor shall completely fill-in all required data fields using the following web address: https://doncmra.nmci.navy.mil/.

Reporting inputs consists of labor hours executed during the contract/TO period of performance within each Government fiscal year (FY) which runs from October 1 through September 30. While inputs may be reported any time during the FY, the contractor shall report all data no later than October 31 of each calendar year. Contractors may direct questions to the help desk at http://www.ecrma.mil/.

5.2.1.5 WAWF Invoicing Notification and Support Documentation
Pursuant to DFARS clause 252.232-7003 and 252.232-7006, the contractor shall submit payment requests and receiving reports using DoD Invoicing, Receipt, Acceptance, and Property Transfer (iRAPT) application (part of the Wide Area Work Flow (WAWF) e-Business Suite) which is a secure Government web-based system for electronic invoicing, receipt, and acceptance. In accordance with clause 252.232-7006, the contractor shall provide e-mail notification to the COR when payment requests are submitted to the iRAPT/WAWF and the contractor shall include cost back–up documentation (e.g., delivery receipts, time sheets, & material/travel costs, etc.) to the invoice in iRAPT/WAWF. As requested, the contractor shall directly provide a soft copy of the invoice and any supporting invoice documentation (CDRL A008) directly to the COR within 24 hours of request to assist in validating the invoiced amount against the products/services provided during the billing cycle.

5.3 EARNED VALUE MANAGEMENT (EVM)

In lieu of EVM, the contractor shall develop and maintain, a Contract Funds Status Report (CDRL A009) to help track Government expenditures against performance.

6.0 QUALITY

6.1 QUALITY SYSTEM

The Contractor's existing approved Quality Assurance Plan shall apply throughout the term of this contract. (CDRL A010)

Upon contract award, the contractor shall maintain a quality assurance process that addresses and meets program objectives in regard to:

- Code development/configured for purpose of capability
- Documentation related to process/procedures and capability
- Application and development of builds for release into the configuration management process while maintaining customer satisfaction focusing on a defect-free products/process.

The contractor shall have a sufficiently documented quality system which contains procedures, planning, and all other documentation and data necessary to provide an efficient and effective quality system based on a contractor's internal auditing system. Thirty (30) days after contract award, the contractor shall provide to the Government a copy of its Quality Assurance Plan (QAP) and any other quality related documents (CDRL A008) as applicable to the TO. The contractor shall make the quality system available to the Government for review at both a program and worksite services level during predetermined visits. Existing quality documents that meet the requirements of this contract may continue to be used. If any quality documentation is disapproved or requires revisions, the contractor shall correct the problem(s) and submit revised documentation NLT 2 weeks after initial disapproval notification. The contractor shall also require all subcontractors to possess a quality assurance and control program commensurate with the services and supplies to be provided as determined by the prime's internal audit system. The Government reserves the right to disapprove the contractor's and/or subcontractor's quality system or portions thereof when the quality system(s) fails to meet contractual requirements at either the program or worksite services level. The Government reserves the right to participate in the process improvement elements of the contractor's quality assurance plan and development of quality related documents as needed. At a minimum, the contractor shall ensure their quality system meets the following key criteria:

- Establish documented, capable, and repeatable processes
- Track issues and associated changes needed
- Monitor and control critical product and process variations
- Establish mechanisms for feedback of field product performance
- Implement and effective root-cause analysis and corrective action system
- Establish methods and procedures for continuous process improvement

6.2 QUALITY MANAGEMENT PROCESS COMPLIANCE

6.2.1 General

The contractor shall have processes in place that coincide with the Government's quality management processes. The contractor shall use best industry practices including, when applicable, ISO/IEC 15288 for System life cycle processes and ISO/IEC 12207 for Software life cycle processes. As applicable, the contractor shall also support and/or participate in event-driven milestones and reviews as stated in the Defense Acquisition University's (DAU's) DoD Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System Chart which is incorporates multiple DoD directives and instructions – specifically DoDD 5000.01 and DoDI 5000.02.

6.3 QUALITY ASSURANCE

The contractor shall perform all quality assurance process audits necessary in the performance of the various tasks as assigned and identified by the respective WBS, POA&M, or quality system, and the contractor shall deliver related quality plan/procedural documents upon request. The Government reserves the right to perform any additional audits deemed necessary to assure that the contractor processes and related services, documents, and material meet the prescribed requirements and to reject any or all processes or related services, documents, and material in a category when noncompliance is established.

6.4 QUALITY CONTROL

The contractor shall perform all quality control inspections necessary in the performance of the various tasks as assigned and identified by the respective WBS, POA&M, or quality system, and the contractor shall submit related quality objective evidence upon request. Quality objective evidence (CDRL A010) includes any of the following as applicable:

- Detailed incoming receipt inspection records
- First article inspection records
- Certificates of Conformance
- Detailed sampling inspection records based upon MIL-STD-1916 (Verification Level III)
- Quality Measurement and Analysis metrics/data

The Government reserves the right to perform any inspections or pull samples as deemed necessary to assure that the contractor provided services, documents, material, and related evidence meet the prescribed requirements and to reject any or all services, documents, and material in a category when nonconformance is established.

6.5 QUALITY MANAGEMENT DOCUMENTATION

In support of the contract's Quality Assurance Surveillance Plan (QASP) and Contractor Performance Assessment Reporting System (CPARS), the contractor shall provide the following document: Contractor CPARS Draft Approval Document (CDAD) Report (CDRL A012) submitted monthly.

7.0 DOCUMENTATION AND DELIVERABLES

7.1 CONTRACT DATA REQUIREMENT LISTINGS (CDRLs)

The following CDRL listing identifies the data item deliverables required under this contract and the applicable section of the PWS for which they are required. Section J includes the DD Form 1423s that itemize each Contract Data Requirements List (CDRL) required under the basic contract. The contractor shall establish a practical and cost-effective system for developing and tracking the required CDRLs generated under each task. The contractor shall not develop any CDRL classified TOP SECRET with SCI.

CDRL#	Description	PWS Reference Paragraph
A001	Program Management Reports, General	3.2.1
A002	Technical/Analysis Reports, General	3.3.3.1, 3.3.9.2, 3.3.10.1.2, 3.3.10.3.2, 3.3.10.4.3
	RESERVED	
A004	Cybersecurity Workforce (CSWF) Report	5.2.1.3
A005	Task Order Status Report (TOSR)	5.2.1.1
A006	Task Order Closeout Report	5.2.1.2
A007	Contractor Manpower Quarterly Status Report (QSR)	5.2.1.4
A008	Invoice Support Documentation	5.2.1.5
A009	Contract Funds Status Report (CFSR)	5.3
A010	Quality Assurance Plan	6.1
	RESERVED	
A012	Contractor CPARS Draft Approval Document (CDAD) Report	6.5

7.2 ELECTRONIC FORMAT

At a minimum, the contractor shall provide deliverables electronically by e-mail; hard copies are only required if requested by the Government. To ensure information compatibility, the contractor shall guarantee all deliverables (i.e., CDRLs), data, correspondence, and etc., are provided in a format approved by the receiving Government representative. The contractor shall provide all data in an editable format compatible with GCSS-MC PMO standard software configuration as specified below. Contractor shall conform to GCSS-MC PMO standards within 30 days of contract award unless otherwise specified. *The initial costs of compliance to the standard software configurations listed below are not chargeable as a direct cost to the Government.*

	Deliverable	**Software to be used**
a.	Word Processing	Microsoft Word
b.	Technical Publishing	PageMaker/Interleaf/SGML/ MSPublisher
c.	Spreadsheet/Graphics	Microsoft Excel
d.	Presentations	Microsoft PowerPoint
e.	2-D Drawings/ Graphics/Schematics (new data products)	Vector (CGM/SVG)
f.	2-D Drawings/ Graphics/Schematics (existing data products)	Raster (CALS Type I, TIFF/BMP, JPEG, PNG)
g.	Scheduling	Microsoft Project
h.	Computer Aid Design (CAD) Drawings	AutoCAD/Visio
i.	Geographic Information System (GIS)	ArcInfo/ArcView

7.3 INFORMATION SYSTEM

7.3.1 Electronic Communication

The contractor shall have broadband Internet connectivity and an industry standard email system for communication with the Government. The contractor shall be capable of Public Key Infrastructure client side authentication to DOD private web servers. Unless otherwise specified, all key personnel on contract shall be accessible by e-mail through individual accounts during all working hours.

7.3.2 Information Security

Pursuant to DoDM 5200.01, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on contract. The contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

7.3.2.1 Safeguards

The contractor shall protect Government information and shall provide compliance documentation validating they are meeting this requirement in accordance with DFARS Clause 252.204-7012. As of the date of contract award no contractor information system as defined by FAR 252.204-7012 supports performance of this contract. The contractor and all utilized subcontractors shall abide by the following safeguards:

(a) Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.

(b) Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

(c) Sanitize media (e.g., overwrite) before external release or disposal.

(d) Encrypt all information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as portable hard drives and digital optical disks, using DoD Authorized Data-at-Rest encryption technology. NOTE: Thumb drives are not authorized for DoD work, storage, or transfer. Use GSA Awarded DAR solutions (GSA # 10359) complying with ASD-NII/DOD-CIO Memorandum, “Encryption of Sensitive Unclassified Data-at-Rest on Mobile Computing Devices and Removable Storage.” The contractor shall ensure all solutions for contractor information systems on which CUI resides as defined by DFAR 252.204-7012 meet FIPS 140-2 compliance requirements.

(e) Limit information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.

(f) Transmit e-mail, text messages, and similar communications using technology and processes that provide the best commercially available level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS). Encrypt organizational wireless connections and use encrypted wireless connection where available when traveling. If encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using at least application-provided password protection level encryption.

(g) Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

(h) Do not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).

(i) Provide protection against computer network intrusions and data exfiltration, minimally including the following:

1. Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.

2. Monitoring and control of inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

3. Prompt application of security-relevant software patches, service packs, and hot fixes.

(j) As applicable, for contractor information systems on which CUI resides, comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, critical program information (CPI), personally identifiable information, export controlled).

(k) Report loss or unauthorized disclosure of information in accordance with contract or agreement requirements and mechanisms.

7.3.2.2 Compliance
Pursuant to DoDM 5200.01, the contractor shall include in their quality processes procedures that are compliant with information security requirements.

8.0 SECURITY

8.1 ORGANIZATION

8.1.1 Security Classification

Classified work shall be performed under this contract and subsequent task orders, if applicable. The Contractor shall have at the time of contract award and prior to commencement of classified work, a SECRET facility security clearance (FCL).
All PWS tasks in Paragraph 3.0 require access to classified information up to the level of SECRET. Clearance is required to access and handle classified and personal personnel material, attend program meetings, and/or work within restricted areas unescorted.

8.1.2 Security Officer

The contractor shall appoint a Facility Security Officer (FSO) to support those contractor personnel requiring access to Government facility/installation and/or access to information technology systems under this contract. The FSO is a key management personnel who is the contractor's main POC for security issues. The FSO shall have a U.S. Government security clearance equal to or higher that the FCL required on this contract. The FSO shall be responsible for tracking the security requirements for all personnel (subcontractors included) utilized on contract. Responsibilities include entering and updating the personnel security related and mandatory training information within the Staffing Plan document, which is an attachment to the task order status report (TOSR) (CDRL A005). FSO shall also update and track data in the Cyber Security Workforce (CSWF) (CDRL A004).

8.2 PERSONNEL

The contractor shall conform to the security provisions of DoDI 5220.22/DoD 5220.22-M - National Industrial Security Program Operating Manual (NISPOM), SECNAVINST 5510.30, DoD 8570.01-M, and the Privacy Act of 1974. The Contractor shall comply with the above and the Privacy Act of 1974 to the extent that such, by their terms, are expressly applicable to the Contractor's delivery of services under this agreement and impose obligations directly upon the Contractor in its role as an information technology services provider with respect to the services performed under this agreement. The Contractor's methodology for compliance with all privacy requirements are as stated in the Contractor's Services Privacy Policy in effect as of the date of award and included at the end of this PWS as Attachment 3. However, the Contractor's policy above shall in no event be construed to avoid or negate any obligation otherwise required by law. In the event of conflict, the statutory language shall prevail. Further, the

Contractor's policy above regarding dispute resolution is not applicable to the Federal Government. Any dispute between the Contractor and Government will be resolved under the Contract Disputes Act and applicable clauses(s) of this contract. Prior to any labor hours being charged on contract, the contractor shall ensure all personnel (including administrative and subcontractor personnel) have obtained and can maintain favorable background investigations at the appropriate level(s) for access required for the contract/task order, and if applicable, are certified/credentialed for the Cybersecurity Workforce (CSWF). A favorable background determination is determined by either a National Agency Check with Inquiries (NACI), National Agency Check with Law and Credit (NACLC), or Single Scope Background Investigation (SSBI) and favorable Federal Bureau of Investigation (FBI) fingerprint checks. Investigations are not necessarily required for personnel performing unclassified work who do not require access to Government installations/facilities, Government IT systems and IT resources, or GCSS-MC PMO information. *Cost to meet these security requirements is not directly chargeable to task order.*

NOTE: If a final determination is made that an individual does not meet or cannot maintain the minimum fitness standard, the contractor shall permanently remove the individual from GCSS-MC PMO facilities, projects, and/or programs. If an individual who has been submitted for a fitness determination or security clearance is "denied" or receives an "Interim Declination," the contractor shall remove the individual from GCSS-MC PMO facilities, projects, and/or programs until such time as the investigation is fully adjudicated or the individual is resubmitted and is approved. All contractor and subcontractor personnel removed from facilities, projects, and/or programs shall cease charging labor hours directly or indirectly on task and contract.

8.2.1 Personnel Clearance

All personnel associated with this contract shall possess a SECRET personnel security clearance (PCL). These programs/tasks include, as a minimum, contractor personnel having the appropriate clearances required for access to classified data as applicable. Prior to starting work on the task, contractor personnel shall have the required clearance granted by the Department of Defense Consolidated Adjudications Facility (DoD CAF) and shall comply with IT access authorization requirements. In addition, contractor personnel shall possess the appropriate IT level of access for the respective task and position assignment as applicable per DoDI 8500.01, DoD Instruction for Cybersecurity. Any future revision to the respective directive and instruction will be applied to the TO level. Contractor personnel shall handle and safeguard any CUI and/or classified information in accordance with appropriate Department of Defense, Navy, and GCSS-MC PMO security regulations. The contractor shall immediately report any security violation to the GCSS-MC PMO Security Management Office, the COR, and Government Project Manager.

8.2.2 Access Control of Contractor Personnel

8.2.2.1 Physical Access to Government Facilities and Installations

Contractor personnel shall physically access Government facilities and installations for purposes of site visitation, supervisory and quality evaluation, work performed within Government spaces (either temporary or permanent), or meeting attendance. Individuals supporting these efforts shall comply with the latest security regulations applicable to the Government facility/installation.

(a) The majority of Government facilities require contractor personnel to have an approved visit request on file at the facility/installation security office prior to access. The contractor shall initiate and submit a request for visit authorization to the COR in accordance with DoD 5220.22-M (NISPOM) not later than one (1) week prior to visit – timeframes may vary at each facility/ installation. For admission to GCSS-MC PMO facilities/installations, the contractor shall forward a visit request to Joint Personnel Adjudication System (JPAS) GCSS-MC PMO for certification of need to know by the specified COR. For visitation to all other govt. locations, the contractor shall forward visit request documentation directly to the on-site facility/installation security office (to be identified at task order level) via approval by the COR.

(b) Depending on the facility/installation regulations, contractor personnel shall present a proper form of identification(s) and vehicle proof of insurance or vehicle rental agreement. NOTE: GCSS-MC PMO facilities require a Common Access Card (CAC) each time physical installation access is required. Contractor shall contact GCSS-MC PMO Security Office directly for latest policy.

(c) All contractor persons engaged in work while on Government property shall be subject to inspection of their vehicles at any time by the Government, and shall report any known or suspected security violations to the Security Department at that location.

8.2.2.2 Identification and Disclosure Requirements
Pursuant to DFARS clause 211.106, Contractors shall take all means necessary to not represent themselves as Government employees.

8.2.2.3 Government Badge Requirements
Some contract personnel shall require a Government issued picture badge. While on Government installations/facilities, contractors shall abide by each site's security badge requirements. Various Government installations are continually updating their security requirements to meet Homeland Security Presidential Directive (HSPD-12) identification standards. Contractors are responsible for obtaining and complying with the latest security identification requirements for their personnel. Contractors shall submit valid paper work (e.g., site visit request, request for picture badge, and/or SF-86 for Common Access Card (CAC)) to the applicable Government security office via the contract COR. The contractor's appointed Security Officer, shall track all personnel holding local Government badges at contract or TO level.

8.2.2.4 Common Access Card (CAC) Requirements
Some Government facilities/installations (e.g., Camp Lejeune, NC) require contractor personnel to have a Common Access Card (CAC) for physical access to the facilities or installations. Contractors supporting work that requires access to any DoD IT/network also requires a CAC. Granting of logical and physical access privileges remains a local policy and business operation function of the local facility. The Contractor is responsible for obtaining the latest facility/installation and IT CAC requirements from the applicable local Security Office. When a CAC is required to perform work, contractor personnel shall be able to meet all of the following security requirements prior to work being performed:

(a) Pursuant to DoD Manual (DoDM-1000.13-M-V1), issuance of a CAC is based on the following four criteria:

1. eligibility for a CAC – to be eligible for a CAC, Contractor personnel's access requirement shall meet one of the following three criteria: (a) individual requires access to multiple DoD facilities or access to multiple non-DoD Federal facilities on behalf of the Government on a recurring bases for a period of 6 months or more, (b) individual requires both access to a DoD facility and access to DoD network on site or remotely, or (c) individual requires remote access to DoD networks that use only the CAC logon for user identification.
2. verification of DoD affiliation from an authoritative data source – CAC eligible personnel must be registered in the Defense Enrollment Eligibility Reporting Systems (DEERS) through either an authoritative personnel data feed from the appropriate Service or Agency or Trusted Associated Sponsorship System (TASS) (formally Contractor Verification System (CVS)).
3. completion of background vetting requirements according to FIPS PUB 201-2 and DoD Regulation 5200.2-R – at a minimum, the completion of Federal Bureau of Investigation (FBI) fingerprint check with favorable results and submission of a National Agency Check with Inquiries (NACI) investigation to the Office of Personnel Management (OPM), or a DoD-determined equivalent investigation. NOTE: Contractor personnel requiring logical access shall obtain and maintain a favorable National Agency Check with Law and Credit (NACLC) investigation. Contractor personnel shall contact the GCSS-MC PMO Security Office to obtain the latest CAC requirements and procedures.
4. Verification of a claimed identity – all contractor personnel shall present two forms of identification in its original form to verify a claimed identity. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 115-0136, Employment Eligibility Verification. Consistent with applicable law, at least one document from the Form I-9 list must be a valid (unexpired) State or Federal Government-issued picture identification (ID). The identity documents will be inspected for authenticity, scanned, and stored in the DEERS.

(b) When a contractor requires logical access to a Government IT system or resource (directly or indirectly), the required CAC will have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-M-V1, CAC PKI certificates will be associated with an official Government issued e-mail address (e.g. .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the GCSS-MC PMO Information Assurance Management (IAM)/ISSM office:

1. For Annual DoD Cybersecurity/IA Awareness training, contractors shall use this site: https://twms.nmci.navy.mil
2. For SAAR form, the contractor shall use DD Form 2875. Contractors can obtain a form from the GCSS-MC PMO.

8.2.2.5 Contractor Check-in and Check-out Procedures

All GCSS-MC PMO contractor personnel requiring or possessing a Government badge and/or CAC for facility and/or IT access shall have a GCSS-MC PMO Government sponsor and be in compliance with the most current version of Contractor Check-in and Check-out Instruction and Forms. At contract award throughout contract completion, the contractor shall provide necessary employee information and documentation for employees hired, transferred, and/or terminated in support of this contract within the required timeframe as cited in the Check-in and Check-out instructions. Contractor's Security Officer shall ensure all contractor employees whose services are no longer required on contract return all applicable Government documents/badges to the appropriate Government representative.

8.2.3 <u>IT Position Categories</u>

Pursuant to DoDI 8500.01, DoD 8570.01-M, SECNAVINST 5510.30, SECNAV M-5239.2, and applicable to unclassified DoD information systems, a designator is assigned to certain individuals that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. As defined in DoD 5200.2-R, SECNAVINST 5510.30 and SECNAV M-5510.30, three basic DoN IT levels/Position categories exist:

- IT-I (Privileged access)
- IT-II (Limited Privileged, sensitive information)
- IT-III (Non-Privileged, no sensitive information)

Note: The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position (as used in DoD 5200.2-R, Appendix 10).

Investigative requirements for each category vary, depending on the role and whether the individual is a U.S. civilian contractor or a foreign national. The Contractor PM shall assist the Government Project Manager or COR in determining the appropriate IT Position Category assignment for all contractor personnel. All required Single-Scope Background Investigation (SSBI), SSBI Periodic Reinvestigation (SSBI-PR), and National Agency Check (NAC) adjudication will be performed Pursuant to DoDI 8500.01 and SECNAVINST 5510.30. Requests for investigation of contractor personnel for fitness determinations or IT eligibility without classified access are submitted by GCSS-MC PMO Security Office, processed by the OPM, and adjudicated by DOD CAF. IT Position Categories are determined based on the following criteria:

8.2.3.1 IT-I Level (Privileged) - Positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain. Personnel whose duties meet the criteria for IT-I Position designation require a favorably adjudication of Single Scope Background Investigation (SSBI) or SSBI-PR. The SSBI or SSBI-PR is updated a minimum of every 5 years. Assignment to designated IT-I positions requires U.S. citizenship unless a waiver request is approved by CNO.

8.2.3.2 IT-II Level (Limited Privileged) - Positions in which the incumbent is responsible for the-direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the IT-II Position level to insure the integrity of the system. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudication of a Position of Trust National Agency Check with Law and Credit (PT/NACLC). Assignment to designated IT-II positions requires U.S. citizenship unless a waiver request is approved by CNO.

8.2.3.3 IT-III Level (Non-privileged) - All other positions involved in computer activities. Incumbent in this position has non-privileged access to one or more DoD information systems/applications or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation require a favorably adjudication of a Position of Trust National Agency Check with Written Inquiries (PT/NACI).

8.2.4 Security Training

Regardless of the contract security level required, the contractor shall be responsible for verifying applicable personnel (including subcontractors) receive all required training. At a minimum, the contractor's designated Security Officer shall track the following information: security clearance information; dates possessing Common Access Cards; issued & expired dates GCSS-MC PMO Badge; Cybersecurity training; Privacy Act training; Personally Identifiable Information (PII) training; Cybersecurity Workforce (CSWF) certifications; etc. The contractor shall educate employees on the procedures for the handling and production of classified material and documents, and other security measures as described in the PWS in accordance with DoD 5220.22-M.

8.2.5 Disclosure of Information

In support of DFARS Clause 252.204-7000, contractor employees shall not discuss or disclose any information provided to them in the performance of their duties to parties other than authorized Government and contractor personnel who have a "need to know". The contractor shall not use any information or documentation developed by the contractor under direction of the Government for other purposes without the consent of the Government Contracting Officer.

8.2.6 Handling of Personally Identifiable Information (PII)

When a contractor, including any subcontractor, is authorized access to Personally Identifiable Information (PII), the contractor shall complete the annual PII training requirements, found at https://twms.nmci.navy.mil, and comply with all privacy protections under the Privacy Act (Clause 52.224-1 and 52.224-2). The contractor shall safeguard PII from theft, loss, and compromise. The contractor shall transmit and dispose of PII in accordance with the latest DON policies. The contractor shall not store any Government PII on their personal computers. The contractor shall mark all developed documentation containing PII information accordingly in either the header or footer of the document: "FOUO – Privacy Sensitive. Any misuse or unauthorized disclosure may result in both criminal and civil penalties." Any unauthorized disclosure of privacy sensitive information through negligence or misconduct can lead to contractor removal or contract termination depending on the severity of the disclosure. Upon discovery of a PII breach, the contractor shall immediately notify the Contracting Officer and COR. Contractors responsible for the unauthorized disclosure of PII shall be held accountable for any costs associated with breach mitigation, including those incurred as a result of having to notify personnel. The Contractor shall comply with all Privacy Act requirements to the extent that by its terms, is expressly applicable to the Contractor's delivery of services under this agreement and imposes obligations directly upon the Contractor in its role as an information technology services provider with respect to the services performed under this agreement. The Contractor's methodology for compliance with all privacy requirements are as stated in the Contractor's Services Privacy Policy in effect as of the date of award and included at the end of this PWS as Attachment 3. However, the Contractor's policy above shall in no event be construed to avoid or negate any obligation otherwise required by law. In the event of conflict, the statutory language shall prevail. Further, the Contractor's policy above regarding dispute resolution is not applicable to the Federal Government. Any dispute between Contractor and Government will be resolved under the Contract Disputes Act and applicable clause(s) of this contract.

8.3 OPERATIONS SECURITY (OPSEC) REQUIREMENTS

Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. Pursuant to DoDD 5205.02E and GCSS-MC PMO's OPSEC program implements requirements in DoD 5205.02-M – OPSEC Program Manual. Note: OPSEC requirements are applicable when contract personnel have access to classified information or unclassified Critical Program Information (CPI)/sensitive information.

8.3.1 Local and Internal OPSEC Requirement
Contractor personnel, including subcontractors if applicable, shall adhere to the OPSEC program policies and practices as cited in the GCSS-MC PMO INSTand existing local site OPSEC procedures. The contractor shall development their own internal OPSEC program specific to the contract and based on GCSS-MC PMO OPSEC requirements. At a minimum, the contractor's program shall identify the current GCSS-MC PMO site OPSEC Officer/Coordinator.

8.3.2 OPSEC Training
Contractor shall track and ensure applicable personnel receive initial and annual OPSEC awareness training. Training may be provided by the Government or a contractor's OPSEC Manager. Contractor training shall, as a minimum, cover OPSEC as it relates to contract work, discuss the Critical Information applicable in the contract/task order, and review OPSEC requirements if working at Government facilities. The contractor shall ensure any training materials developed by the contractor shall be reviewed by the GCSS-MC PMO OPSEC Officer, who will ensure it is consistent with GCSS-MC PMO OPSEC policies. OPSEC training requirements are applicable for personnel during their entire term supporting GCSS-MC PMO contracts.

8.3.3 GCSS-MC PMO OPSEC Program
Contractor shall participate in GCSS-MC PMO OPSEC program briefings and working meetings, and the contractor shall complete any required OPSEC survey or data call within the timeframe specified.

8.3.4 Classified Contracts
OPSEC requirements identified under a classified contract shall have specific OPSEC requirements listed on the DD Form 254.

8.4 DATA HANDLING AND USER CONTROLS

8.4.1 Data Handling
At a minimum, the contractor shall handle all data received or generated under this contract as For Official Use Only (FOUO) material. The contractor shall handle all classified information received or generated Pursuant to the attached DD Form 254 and be in compliance with all applicable PWS references and other applicable Government policies and procedures that include DOD/Navy/ GCSS-MC PMO.

8.4.2 Effective Use of Controls
The contractor shall screen all electronic deliverables or electronically provided information for malicious code using DoD approved anti-virus software prior to delivery to the Government. The contractor shall utilize appropriate controls (firewalls, password protection, encryption, digital certificates, etc.) at all times to protect contract related information processed, stored or transmitted on the contractor's and Government's computers/servers to ensure confidentiality, integrity, availability, authentication and non-repudiation. The contractor shall ensure provisions are in place that will safeguard all aspects of information operations pertaining to this contract in compliance with all applicable PWS references. In compliance with Para 7.3.2.1, the contractor shall ensure Data-at-Rest is required on all portable electronic devices including storage of all types. Encryption/digital signing of communications is required for authentication and non-repudiation.

9.0 GOVERNMENT FACILITIES

As specified in each task order, Government facilities (i.e., office space, computer hardware/software, or lab space) will be provided to those labor categories that would otherwise adversely affect the work performance if they were not available on-site. All Contractor personnel with supplied Government facilities shall be located GCSS-MC PMO offices located at 105 Tech Parkway, Stafford, VA.

10.0 RESERVED

11.0 RESERVED

12.0 SAFETY ISSUES

12.1 OCCUPATIONAL SAFETY AND HEALTH REQUIREMENTS

The contractor shall be responsible for ensuring the safety of all company employees, other working personnel, and Government property. The contractor is solely responsible for compliance with those applicable Occupational Safety and Health Act (OSHA) (Public Law 91-596) and the resulting applicable standards, OSHA Standard 29 CFR 1910 (general), 1915 (shipboard/submarine) and 1926 (shore), and for the protection, safety and health of their employees and any subcontractors assigned to the respective task orders under this contract. Without government assistance, the contractor shall make certain that all safety requirements are met, safety equipment is provided, and safety procedures are documented as part of their quality management system.

12.1.1 Performance at Government Facilities
The Contractor shall as soon as reasonably possible report any accidents involving government or Contractor personnel injuries or property/equipment damage to the contracting officer and COR. Additionally, the Contractor is responsible for securing the scene and impounding evidence/wreckage until released by the contracting officer.

13.0 TRAVEL

13.1 LOCATIONS

The majority of the work under this contract shall be performed at the Contractor's location and Government places of visit. Related travel inclusive of lodging and transportation for CONUS locations shall be in accordance with Joint Travel Regulations. As specified at the task order level, travel shall be required, at a minimum, to the following locations:

1) PMO offices located at 105 Tech Parkway in Stafford, VA
2) SDE at Carpathia in Reston VA
3) SSC-A-Charleston, SC
4) SSC-A-Norfolk, VA
5) SSC-A-NOLA New Orleans, LA
6) Mechanicsburg, PA
7) St. Louis, MO
8) MCB Quantico, VA
9) MCLB Albany, GA
10) Camp Lejeune, NC
11) Camp Pendleton, CA, and BIC
12) Jacksonville, FL

Note: Under this contract and any subsequent task orders, the contractor shall not travel to Afghanistan.

14.0 ACCEPTANCE PLAN

Inspection and acceptance is performed by the COR on all services, data, and non-data deliverables in accordance with the Quality Assurance Surveillance Plan (QASP), Attachment 2.

15.0 RESERVED

16.0 RESERVED

(End of PWS)

Exhibit/Attachment Table of Contents

<u>DISTRIBUTION</u>

<u>Contractor:</u> Oracle America Incorporated 5000 Oracle Pkwy Redwood City, CA 94065-1677	DFAS-CO/WEST ENTITLEMENT OPS (HQ0339) DCMA LATHROP (S0507A)
	GOVERNMENT CODES: Contracting Officer's Representative: (b)(6) Email: (b)(6) @usmc.mil Telephone: (703) 432-(b)(6) Contracting Officer: Mr. Jesse R. Seaton Email: jesse.seaton@navy.mil Telephone: 843-218-4146 Contract Administrator: TBD